Distributed Detection and Estimation in Wireless Sensor Networks: Resource Allocation, Fusion Rules, and Network Security

Edmond Nurellari

The University of Leeds, UK
School of Electronic and Electrical Engineering

In accordance with the requirements for the degree of Doctor of Philosophy

June 6, 2017

Overview

Overview

Overview

Overview

Overview

Overview

Overview

Overview

1. Introduction

Motivation

- WSNs spatially deployed over a field can be designed to collect information and monitor many phenomena of interest.

1. Introduction

Motivation

- WSNs spatially deployed over a field can be designed to collect information and monitor many phenomena of interest.
- Important role in several daily application scenarios such as health-care monitoring, home applications, smart farming, environment monitoring, and military.

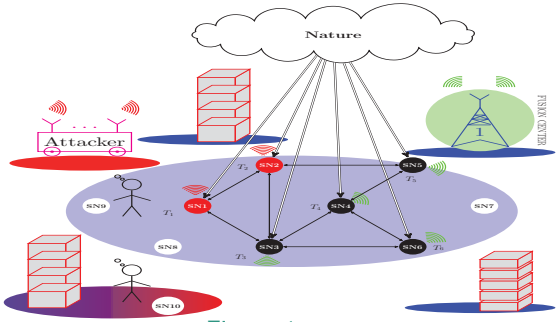

Figure 1: (left) A WSN architecture. (right) Smart city infrastructure.

1. Introduction

Motivation

- WSNs spatially deployed over a field can be designed to collect information and monitor many phenomena of interest.
- Important role in several daily application scenarios such as health-care monitoring, home applications, smart farming, environment monitoring, and military.

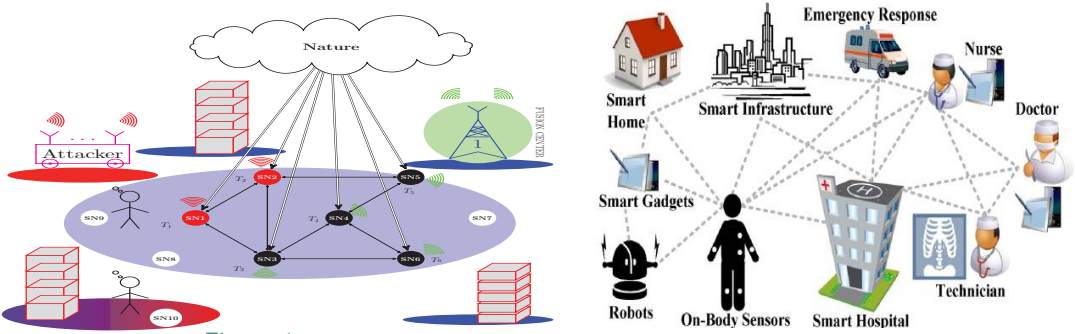

Figure 1: (left) A WSN architecture. (right) Smart city infrastructure.

Design Challenges in WSNs

- Low Power Hardware: Clearly, the biggest design constraint in WSNs still remains the power consumption. Even-though the SNs are being designed using low-power micro controllers, their power dissipation is still orders of magnitude too high.

Design Challenges in WSNs

- Low Power Hardware: Clearly, the biggest design constraint in WSNs still remains the power consumption. Even-though the SNs are being designed using low-power micro controllers, their power dissipation is still orders of magnitude too high.

- Resource Constraints: Battery operated devices with limited on-board energy, both the system lifetime and communication bandwidth (BW) are restricted. Both the signal processing and communication should be carefully designed to consume minimal energy in order to extend the lifetime and improve the overall reliability of the WSN.

Design Challenges in WSNs

- Low Power Hardware: Clearly, the biggest design constraint in WSNs still remains the power consumption. Even-though the SNs are being designed using low-power micro controllers, their power dissipation is still orders of magnitude too high.

- Resource Constraints: Battery operated devices with limited on-board energy, both the system lifetime and communication bandwidth (BW) are restricted. Both the signal processing and communication should be carefully designed to consume minimal energy in order to extend the lifetime and improve the overall reliability of the WSN.

- Network Security:Usually unattended (geographically dispersed) and this makes them vulnerable to attacks. The overall detection and estimation strongly depends on the reliability of these SNs.

Contribution-Publications List

1. **E. Nurellari**, D. McLernon, and M. Ghogho "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks", in *IEEE Trans. on Signal and Information Processing over Networks (TSIPN), April 2017*.

Contribution-Publications List

1. **E. Nurellari**, D. McLernon, and M. Ghogho "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks", in *IEEE Trans. on Signal and Information Processing over Networks (TSIPN), April 2017*.
2. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation", in *IEEE Sensors Journal*, vol. 16, no. 16, pp. 6298-6309, Aug. 15, 2016.

Contribution-Publications List

1. **E. Nurellari**, D. McLernon, and M. Ghogho "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks", in *IEEE Trans. on Signal and Information Processing over Networks (TSIPN), April 2017*.
2. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation", in *IEEE Sensors Journal*, vol. 16, no. 16, pp. 6298-6309, Aug. 15, 2016.
3. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Two-Step Quantized Fusion Rules via Consensus Algorithm for Distributed Detection in Wireless Sensor Networks," in *IEEE Transactions on Signal and Information Processing over Networks (TSIPN)*, vol. 2, no. 3, pp. 321-335, Sept. 2016.

Contribution-Publications List

1. **E. Nurellari**, D. McLernon, and M. Ghogho "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks", in *IEEE Trans. on Signal and Information Processing over Networks (TSIPN), April 2017*.
2. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation", in *IEEE Sensors Journal*, vol. 16, no. 16, pp. 6298-6309, Aug. 15, 2016.
3. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Two-Step Quantized Fusion Rules via Consensus Algorithm for Distributed Detection in Wireless Sensor Networks," in *IEEE Transactions on Signal and Information Processing over Networks (TSIPN)*, vol. 2, no. 3, pp. 321-335, Sept. 2016.
4. S. Aldalahmeh, M. Ghogho, D. McLernon, and **E. Nurellari**, "Optimal fusion rule for distributed detection in clustered wireless sensor networks", *EURASIP Journal on Advances in Signal Process.*, 2016:5, Jan. 2016.

Contribution-Publications List

1. **E. Nurellari**, D. McLernon, and M. Ghogho "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks", in *IEEE Trans. on Signal and Information Processing over Networks (TSIPN), April 2017*.
2. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation", in *IEEE Sensors Journal*, vol. 16, no. 16, pp. 6298-6309, Aug. 15, 2016.
3. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Two-Step Quantized Fusion Rules via Consensus Algorithm for Distributed Detection in Wireless Sensor Networks," in *IEEE Transactions on Signal and Information Processing over Networks (TSIPN)*, vol. 2, no. 3, pp. 321-335, Sept. 2016.
4. S. Aldalahmeh, M. Ghogho, D. McLernon, and **E. Nurellari**, "Optimal fusion rule for distributed detection in clustered wireless sensor networks", *EURASIP Journal on Advances in Signal Process.*, 2016:5, Jan. 2016.
5. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed detection in practical wireless sensor networks via a two step consensus algorithm," in *Proc. IET Int. conf. on Intelligent Signal Process. (ISP)*, London, United Kingdom, 1-2 Dec. 2015.

Contribution-Publications List

1. **E. Nurellari**, D. McLernon, and M. Ghogho "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks", in *IEEE Trans. on Signal and Information Processing over Networks (TSIPN), April 2017*.
2. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation", in *IEEE Sensors Journal*, vol. 16, no. 16, pp. 6298-6309, Aug. 15, 2016.
3. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Two-Step Quantized Fusion Rules via Consensus Algorithm for Distributed Detection in Wireless Sensor Networks," in *IEEE Transactions on Signal and Information Processing over Networks (TSIPN)*, vol. 2, no. 3, pp. 321-335, Sept. 2016.
4. S. Aldalahmeh, M. Ghogho, D. McLernon, and **E. Nurellari**, "Optimal fusion rule for distributed detection in clustered wireless sensor networks", *EURASIP Journal on Advances in Signal Process.*, 2016:5, Jan. 2016.
5. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed detection in practical wireless sensor networks via a two step consensus algorithm," in *Proc. IET Int. conf. on Intelligent Signal Process. (ISP)*, London, United Kingdom, 1-2 Dec. 2015.
6. **E. Nurellari**, D. McLernon, M. Ghogho and S. A. R. Zaidi, "Distributed Optimal Quantization and Power Allocation for Sensor Detection Via Consensus," *Proc. IEEE VTC Spring*, Glasgow, U.K., 11-14 May 2015.

Contribution-Publications List

1. **E. Nurellari**, D. McLernon, and M. Ghogho "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks", in *IEEE Trans. on Signal and Information Processing over Networks (TSIPN), April 2017*.
2. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation", in *IEEE Sensors Journal*, vol. 16, no. 16, pp. 6298-6309, Aug. 15, 2016.
3. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Two-Step Quantized Fusion Rules via Consensus Algorithm for Distributed Detection in Wireless Sensor Networks," in *IEEE Transactions on Signal and Information Processing over Networks (TSIPN)*, vol. 2, no. 3, pp. 321-335, Sept. 2016.
4. S. Aldalahmeh, M. Ghogho, D. McLernon, and **E. Nurellari**, "Optimal fusion rule for distributed detection in clustered wireless sensor networks", *EURASIP Journal on Advances in Signal Process.*, 2016:5, Jan. 2016.
5. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed detection in practical wireless sensor networks via a two step consensus algorithm," in *Proc. IET Int. conf. on Intelligent Signal Process. (ISP)*, London, United Kingdom, 1-2 Dec. 2015.
6. **E. Nurellari**, D. McLernon, M. Ghogho and S. A. R. Zaidi, "Distributed Optimal Quantization and Power Allocation for Sensor Detection Via Consensus," *Proc. IEEE VTC Spring*, Glasgow, U.K., 11-14 May 2015.
7. **E. Nurellari**, S. Aldalahmeh, M. Ghogho, and D. McLernon, "Quantized Fusion Rules for Energy-Based Distributed Detection in Wireless Sensor Networks," *Proc. IEEE SSPD*, Edinburgh, Scotland, 8-9 Sep. 2014.

Contribution-Publications List

1. **E. Nurellari**, D. McLernon, and M. Ghogho "A Secure Optimum Distributed Detection Scheme in Under-Attack Wireless Sensor Networks", in *IEEE Trans. on Signal and Information Processing over Networks (TSIPN), April 2017*.
2. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Binary Event Detection Under Data-Falsification and Energy-Bandwidth Limitation", in *IEEE Sensors Journal*, vol. 16, no. 16, pp. 6298-6309, Aug. 15, 2016.
3. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed Two-Step Quantized Fusion Rules via Consensus Algorithm for Distributed Detection in Wireless Sensor Networks," in *IEEE Transactions on Signal and Information Processing over Networks (TSIPN)*, vol. 2, no. 3, pp. 321-335, Sept. 2016.
4. S. Aldalahmeh, M. Ghogho, D. McLernon, and **E. Nurellari**, "Optimal fusion rule for distributed detection in clustered wireless sensor networks", *EURASIP Journal on Advances in Signal Process.*, 2016:5, Jan. 2016.
5. **E. Nurellari**, D. McLernon, and M. Ghogho, "Distributed detection in practical wireless sensor networks via a two step consensus algorithm," in *Proc. IET Int. conf. on Intelligent Signal Process. (ISP)*, London, United Kingdom, 1-2 Dec. 2015.
6. **E. Nurellari**, D. McLernon, M. Ghogho and S. A. R. Zaidi, "Distributed Optimal Quantization and Power Allocation for Sensor Detection Via Consensus," *Proc. IEEE VTC Spring*, Glasgow, U.K., 11-14 May 2015.
7. **E. Nurellari**, S. Aldalahmeh, M. Ghogho, and D. McLernon, "Quantized Fusion Rules for Energy-Based Distributed Detection in Wireless Sensor Networks," *Proc. IEEE SSPD*, Edinburgh, Scotland, 8-9 Sep. 2014.
8. **E. Nurellari**, D. McLernon, M. Ghogho and S. Aldalahmeh, "Optimal quantization and power allocation for energy-based distributed sensor detection," *Proc. IEEE EUSIPCO*, Lisbon, Portugal, 1-5 Sept. 2014.

Overview

2. Optimal Quantization and Power Allocation

System Architecture

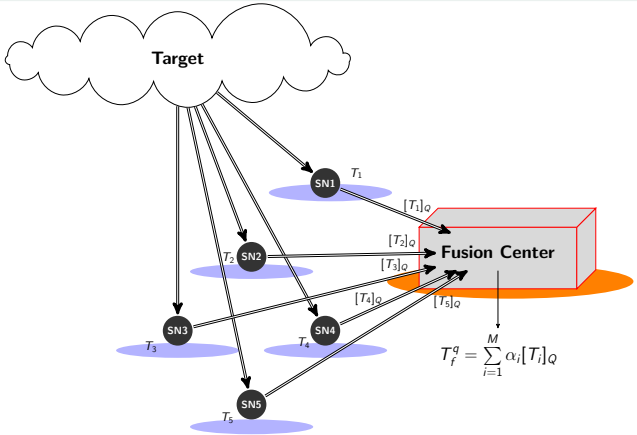

Figure 2: Communication architecture between peripheral SNs and the FC. Each SN generates a test statistic by observing the target and can communicate with the FC only over an energy-constrained/bandwidth-constrained link.

2. Simulation Results 1/2

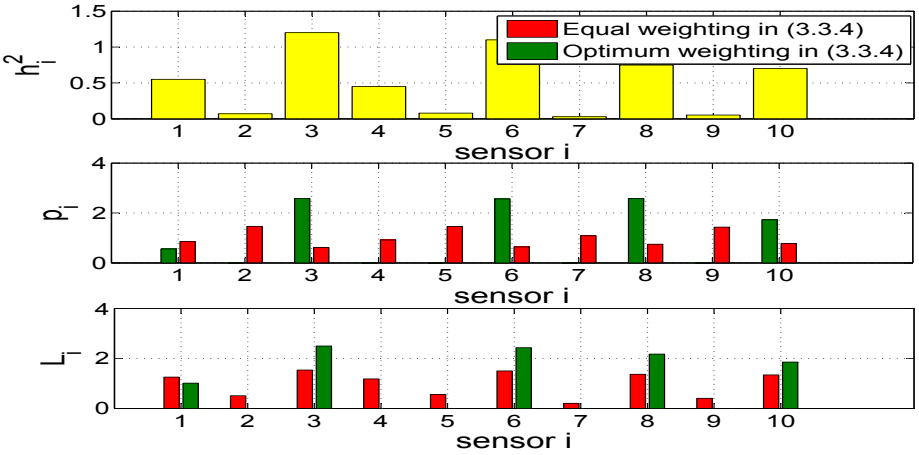

Figure 3: Equal weight ($\alpha_i = \frac{1}{\sqrt{M}}, \forall i$) and optimal weight combining ($\boldsymbol{\alpha} = \boldsymbol{\alpha}_{opt}$) transmit power and channel quantization bits allocation for $P_{fa} = 0.1$, $P_t = 10$, $U = 0.1$, and $M = 10$.

2. Simulation Results 2/2

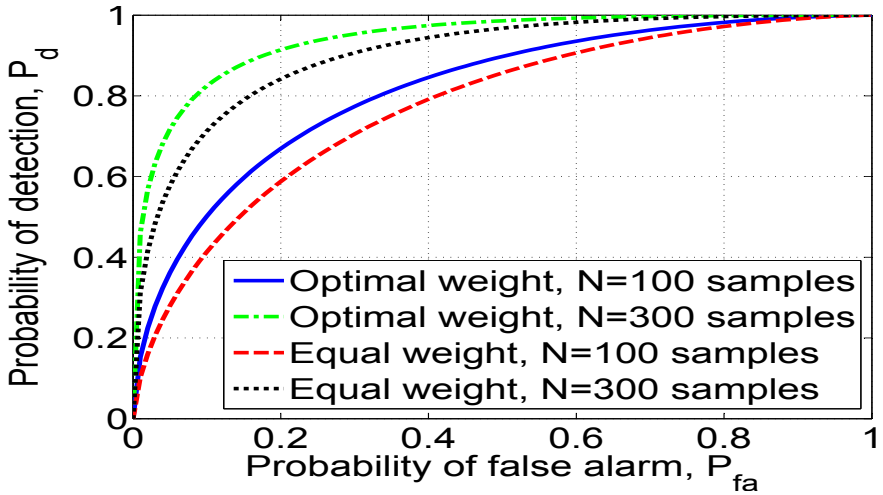

Figure 4: Receiver operating characteristic with $P_t = 10$, $U = 0.1$ and $M = 10$ for two different weighting schemes.

Overview

3. Simulation Results 1/3

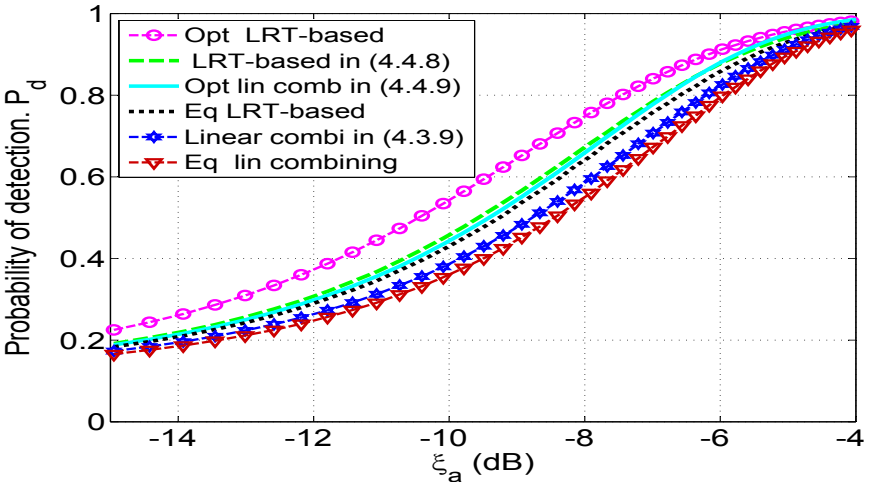

Figure 5: Probability of detection (P_d) versus the signal to noise ratio (ξ_a) for $M = 20$, $N = 10$, $P_t = 10$, $P_{fa} = 0.1$ and $B = 0.5$.

3. Simulation Results 2/3

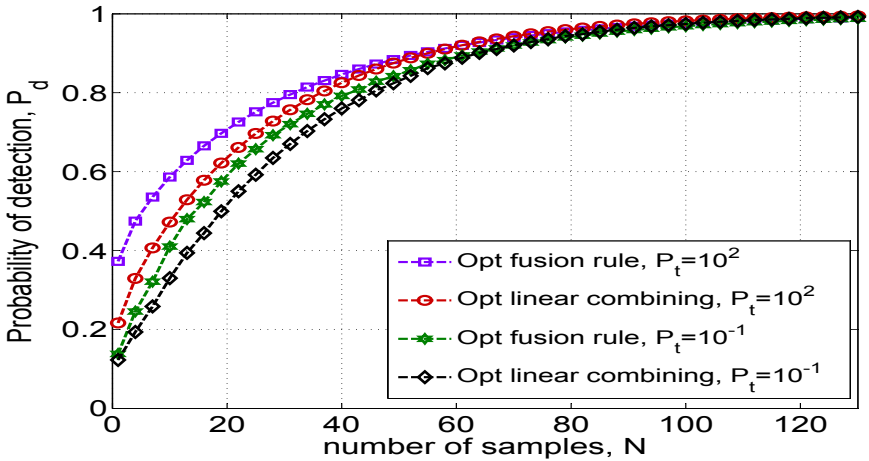

Figure 6: Probability of detection (P_d) versus the number of samples (N) for $M = 10$ sensors, $P_{fa} = 0.1$, $\xi_a = -8.5$ dB and $B = 1$.

3. Simulation Results 3/3

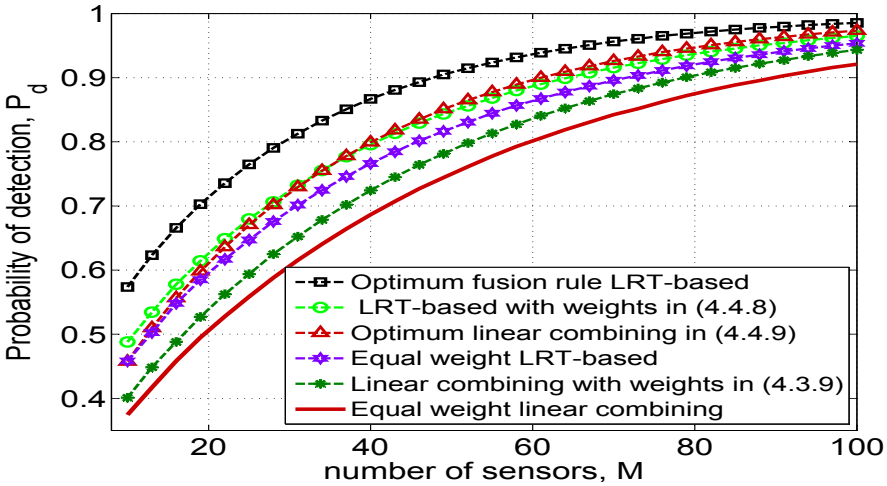

Figure 7: Probability of detection (P_d) versus number of sensors (M) for $N = 10$, $P_t = 10$, $P_{fa} = 0.1$, $\xi_a = -8.5$ dB and $B = 0.5$.

Overview

4. Distributed Two-Step Quantized Fusion Rules

Communication Architecture

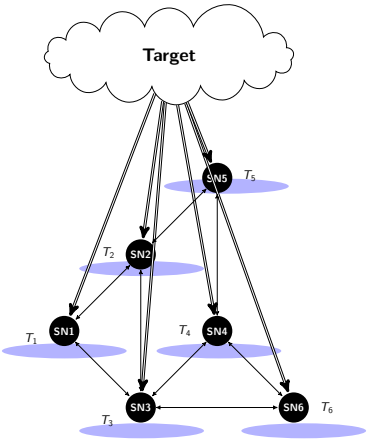

Figure 8: A distributed communication architecture among peripheral SNs. The SNs have partial connectivity (thin lines) among themselves (i.e., not a complete graph).

4. Quantized Distributed Soft Decision Fusion Rule

Proposition

- Here we propose a scheme, where SN i encodes the data (using a simple uniform quantizer with q_i bits) prior to information exchange.

4. Quantized Distributed Soft Decision Fusion Rule

Proposition

- Here we propose a scheme, where SN i encodes the data (using a simple uniform quantizer with q_i bits) prior to information exchange.

1. We also propose to establish a link between any two SNs i and j based on the (known) SNR at node j, i.e.

$$\left.\begin{array}{l} \text{if } SNR_{ij} < \Upsilon,\ e_{ij} = e_{ji} = 0 \\ \text{if } SNR_{ij} \geq \Upsilon,\ e_{ij} = e_{ji} = 1. \end{array}\right\}$$

4. Quantized Distributed Soft Decision Fusion Rule

Proposition

- Here we propose a scheme, where SN i encodes the data (using a simple uniform quantizer with q_i bits) prior to information exchange.

1. We also propose to establish a link between any two SNs i and j based on the (known) SNR at node j, i.e.

$$\left.\begin{array}{l} \text{if } SNR_{ij} < \Upsilon,\ e_{ij} = e_{ji} = 0 \\ \text{if } SNR_{ij} \geq \Upsilon,\ e_{ij} = e_{ji} = 1. \end{array}\right\}$$

2. Υ is a SNR threshold parameter and SNR_{ij} defined as:

$$SNR_{ij} = \frac{p_{ij}^t h_{ij}^2}{\zeta_0 d_{ij}^{\gamma}}.$$

4. Quantized Distributed Soft Decision Fusion Rule

Proposition

- We propose to quantize with q_i bits at SN i before transmitting to SN j :

$$q_i \leq \frac{1}{2}\log_2\left(1+\Upsilon\right) \qquad \text{bits/sample}$$

4. Quantized Distributed Soft Decision Fusion Rule

Proposition

- We propose to quantize with q_i bits at SN i before transmitting to SN j :

$$q_i \leq \frac{1}{2}\log_2\left(1+\Upsilon\right) \qquad \text{bits/sample}$$

- A large Υ means:
  1. Fewer communication links and so slower information diffusion across the network.

4. Quantized Distributed Soft Decision Fusion Rule

Proposition

- We propose to quantize with q_i bits at SN i before transmitting to SN j :

$$q_i \leq \frac{1}{2}\log_2(1+\Upsilon) \qquad \text{bits/sample}$$

- A large Υ means:
  1. Fewer communication links and so slower information diffusion across the network.
  2. An increase in the number of bits that each SN can transmit to its neighbors.

4. Quantized Distributed Soft Decision Fusion Rule

Proposition

- We propose to quantize with q_i bits at SN i before transmitting to SN j :

$$q_i \leq \frac{1}{2}\log_2(1+\Upsilon) \qquad \text{bits/sample}$$

- A large Υ means:
  1. Fewer communication links and so slower information diffusion across the network.
  2. An increase in the number of bits that each SN can transmit to its neighbors.
- A small Υ means:
  1. Establishes a more connected graph and dictates a faster information diffusion across the network.

4. Quantized Distributed Soft Decision Fusion Rule

Proposition

- We propose to quantize with q_i bits at SN i before transmitting to SN j :

$$q_i \leq \frac{1}{2}\log_2(1+\Upsilon) \qquad \text{bits/sample}$$

- A large Υ means:
  1. Fewer communication links and so slower information diffusion across the network.
  2. An increase in the number of bits that each SN can transmit to its neighbors.
- A small Υ means:
  1. Establishes a more connected graph and dictates a faster information diffusion across the network.
  2. Allows less transmission bits resulting in an increase in the quantization noise variance.

4. Simulation Results 1/6

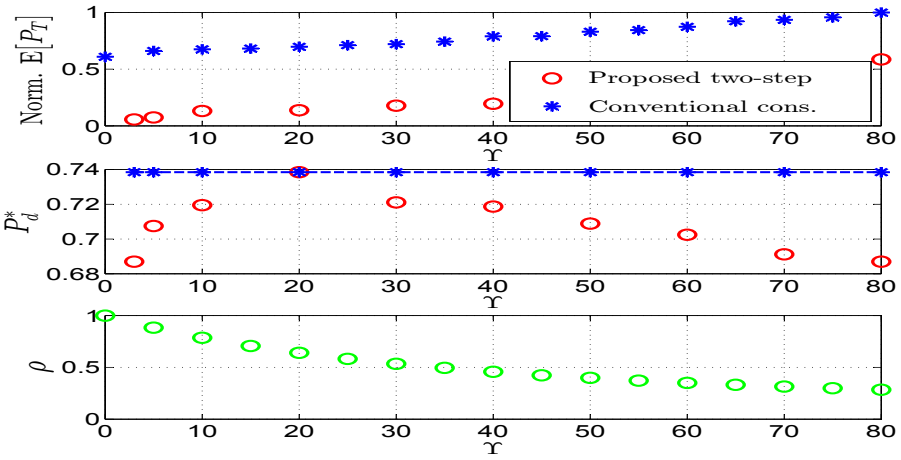

Figure 9: Normalized average power consumption ($\mathbb{E}[P_T]$), achievable[8] probability of detection (P_d^*) and the average communication link density (ρ) versus Υ, with $\sigma_{e_h}^2 = 0$, decision fusion in (5.4.16), $P_{fa}^g = 0.1$, $U = 3$, $N = 20$, $M = 17$ and with α_i (scaled by M).

4. Simulation Results 2/6

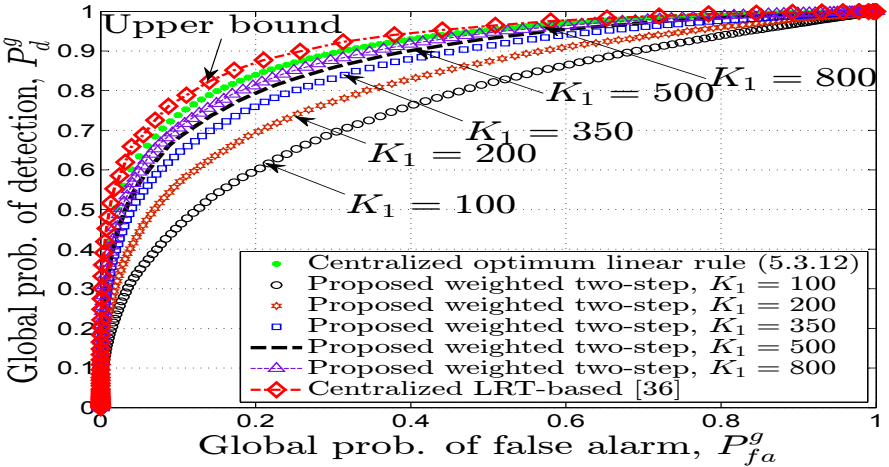

Figure 10: Averaged (over 500 h_{ij}^2 realizations) ROC for the proposed two-step weighted algorithm with decision fusion in (40), $U = 3$, $N = 20$, $M = 17$, $K_2 = 3$, $\Upsilon = 30$, $\sigma_{e_h}^2 = 0$ and with α_i (scaled by M) in (5.3.9).

4. Simulation Results 3/6

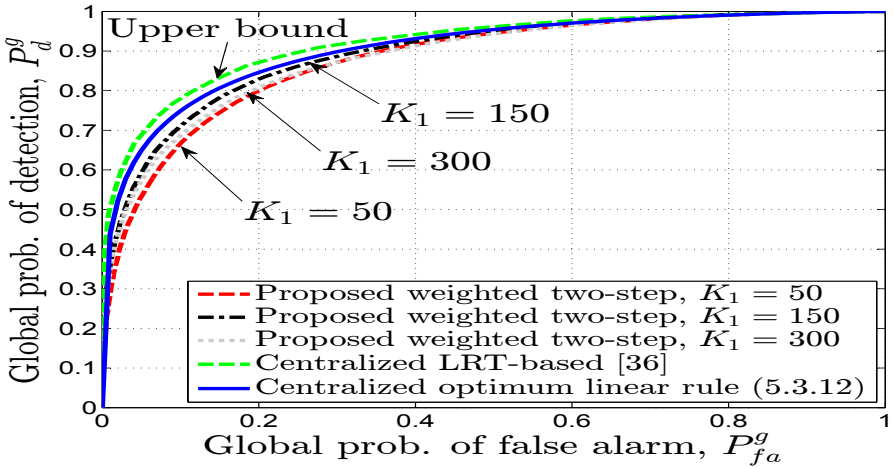

Figure 11: Averaged (over 500 h_{ij}^2 realizations) ROC against first step iterations number (K_1), with decision fusion in (41), $K_2 = 2$, $U = 3$, $N = 20$, $M = 17$, $\Upsilon = 10$, $\sigma_{e_h}^2 = 0$ and with α_i (scaled by M) in (5.3.9).

4. Simulation Results 4/6

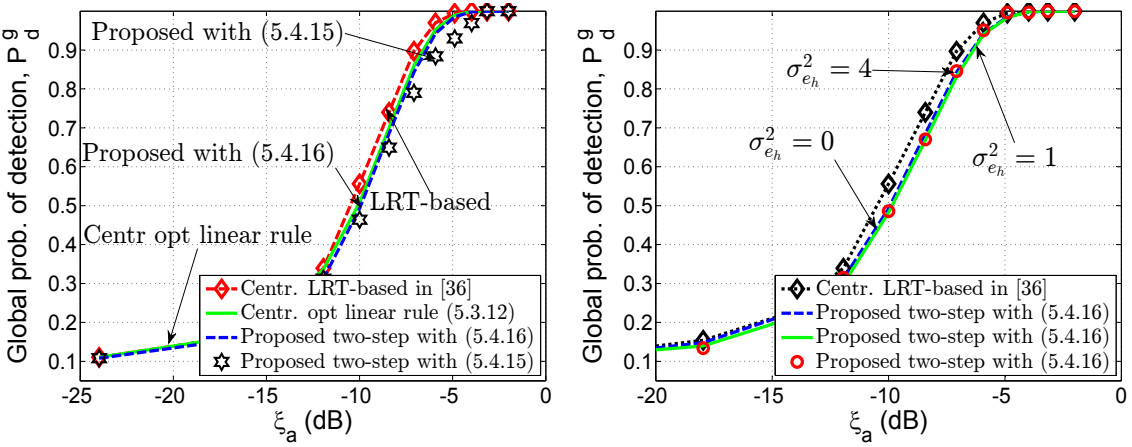

Figure 12: Averaged (over 500 h_{ij}^2 realizations) probability of detection (P_d^g) against the signal to noise ratio (ξ_a) with $P_{fa}^g = 0.1$, $U = 3$, $N = 20$, $M = 17$, $K_1 = 320$, $\Upsilon = 20$, $\xi_i = \xi, \forall i$ in (4) and with α_i (scaled by M) in (5.3.9): (left) ideal, $\sigma_{e_h}^2 = 0$; (right) non-ideal, $\sigma_{e_h}^2 \neq 0$.

4. Simulation Results 5/6

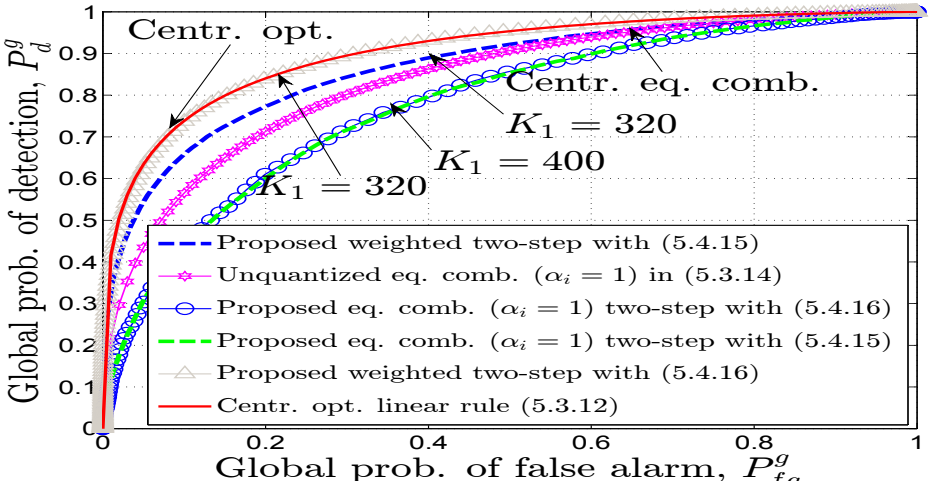

Figure 13: Averaged (over 500 h_{ij}^2 realizations) ROC for the proposed (quantized) two-step weighted fusion rule with $U = 3$, $N = 20$, $\Upsilon = 20$, $M = 17$ and with α_i (scaled by M) in (5.3.9).

4. Simulation Results 6/6

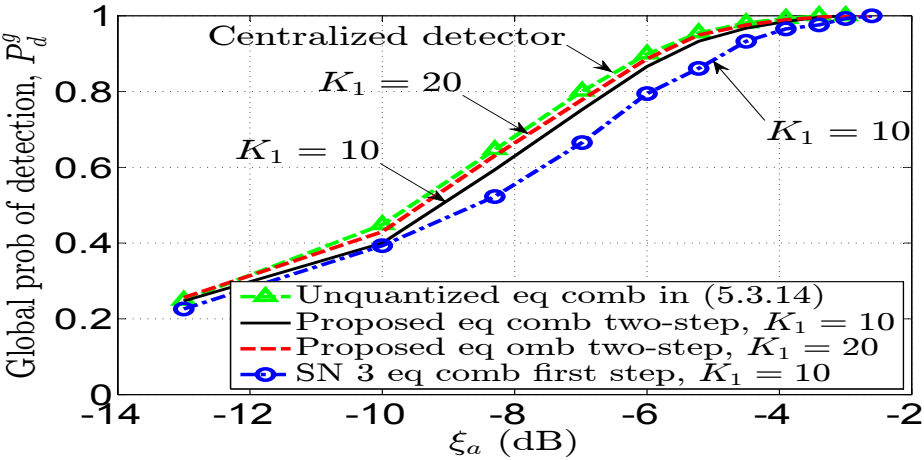

Figure 14: Probability of detection (P_d^g) versus the signal to noise ratio (ξ_a) for $M = 13$, $\Upsilon = 72$, $U = 2$, $N = 20$, $P_{fa}^g = 0.1$ and $\xi_i = \xi . \forall i$ in (3.2.4) and $\alpha_i = 1, \forall i$ in (5.4.4). The topology used is given in right of Fig. 5.5.

Overview

5. Sensor Detection in the Presence of Falsified Observations

Motivation

1. Geographically dispersed to cover large areas, the SNs are constrained in both bandwidth and power. Usually unattended and this makes them vulnerable to different attacks.

Contributions

5. Sensor Detection in the Presence of Falsified Observations

Motivation

1. Geographically dispersed to cover large areas, the SNs are constrained in both bandwidth and power. Usually unattended and this makes them vulnerable to different attacks.
2. The overall detection performance strongly depends on the reliability of these SNs in the network.

Contributions

5. Sensor Detection in the Presence of Falsified Observations

Motivation

1. Geographically dispersed to cover large areas, the SNs are constrained in both bandwidth and power. Usually unattended and this makes them vulnerable to different attacks.
2. The overall detection performance strongly depends on the reliability of these SNs in the network.
3. While fusing the data received by the spatially deployed SNs allows the FC to make a reliable decision, it is possible that one or more SNs (compromised by an attacker) deliberately falsify their local observations.

Contributions

5. Sensor Detection in the Presence of Falsified Observations

Motivation

1. Geographically dispersed to cover large areas, the SNs are constrained in both bandwidth and power. Usually unattended and this makes them vulnerable to different attacks.
2. The overall detection performance strongly depends on the reliability of these SNs in the network.
3. While fusing the data received by the spatially deployed SNs allows the FC to make a reliable decision, it is possible that one or more SNs (compromised by an attacker) deliberately falsify their local observations.

Contributions

1. The problem of centralized detection in the presence of compromised SNs is investigated.

5. Sensor Detection in the Presence of Falsified Observations

Motivation

1. Geographically dispersed to cover large areas, the SNs are constrained in both bandwidth and power. Usually unattended and this makes them vulnerable to different attacks.
2. The overall detection performance strongly depends on the reliability of these SNs in the network.
3. While fusing the data received by the spatially deployed SNs allows the FC to make a reliable decision, it is possible that one or more SNs (compromised by an attacker) deliberately falsify their local observations.

Contributions

1. The problem of centralized detection in the presence of compromised SNs is investigated.
2. Attacker-based and FC-based parameter optimization are considered and some expressions have been derived.

5. Sensor Detection in the Presence of Falsified Observations

Motivation

1. Geographically dispersed to cover large areas, the SNs are constrained in both bandwidth and power. Usually unattended and this makes them vulnerable to different attacks.
2. The overall detection performance strongly depends on the reliability of these SNs in the network.
3. While fusing the data received by the spatially deployed SNs allows the FC to make a reliable decision, it is possible that one or more SNs (compromised by an attacker) deliberately falsify their local observations.

Contributions

1. The problem of centralized detection in the presence of compromised SNs is investigated.
2. Attacker-based and FC-based parameter optimization are considered and some expressions have been derived.
3. A reputation based scheme to identify the compromised SNs in the network and control their influence to the global FC decision is also proposed.

5. Sensor Detection in the Presence of Falsified Observations

Communication Architecture

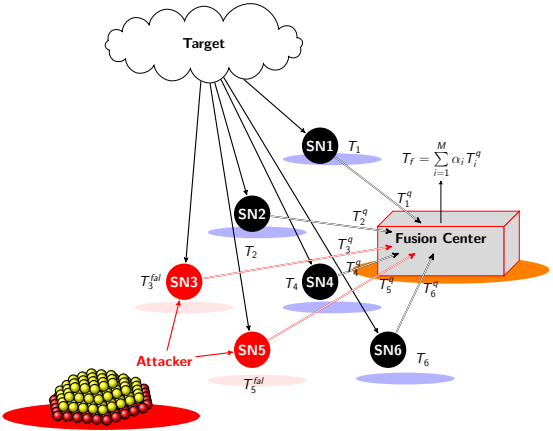

Figure 15: Under attack communication architecture between peripheral SNs and the FC. While the honest SNs test statistics remain unchanged, the compromised SNs falsify their test statistics before transmitting to the FC.

5. Simulation Results 1/4

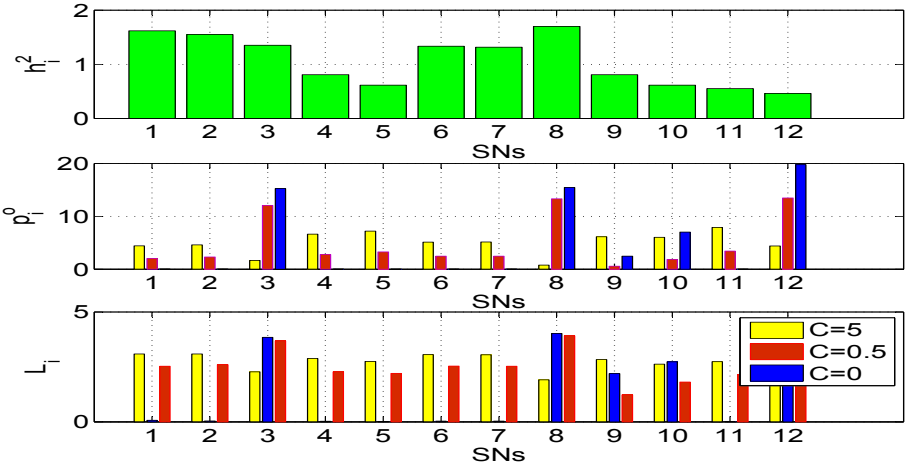

Figure 16: SN optimal transmit power (p_i^o) and channel bit allocation (L_i) with $P_t = 60$, $U = 3$, $\xi_a = -10.5$ dB, $N = 20$, $\beta = 0.1$ and $\sigma^2_{e_h} = 0$.

5. Simulation Results 2/4

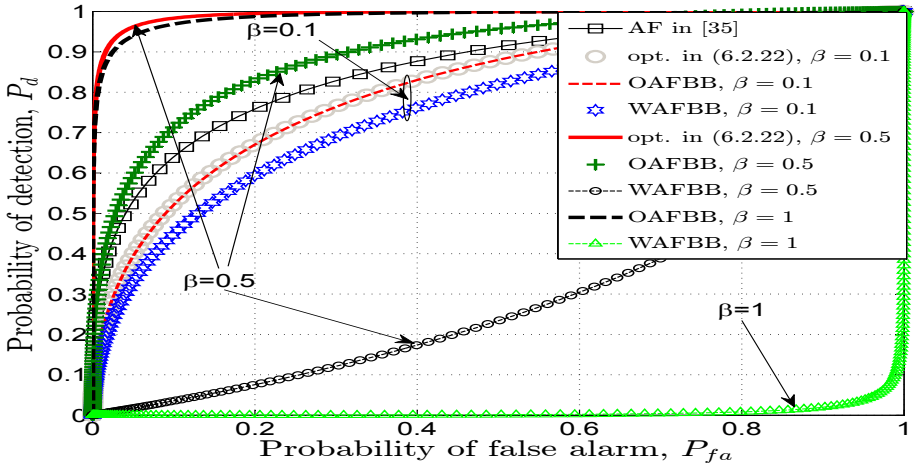

Figure 17: Probability of detection (P_d) versus probability of false alarm (P_{fa}) with $U = 3$, $P_t = 60$, $M = 12$, $N = 20$, $C_i = 0.9, \forall i$ and $\sigma^2_{e_h} = 0$.

5. Simulation Results 3/4

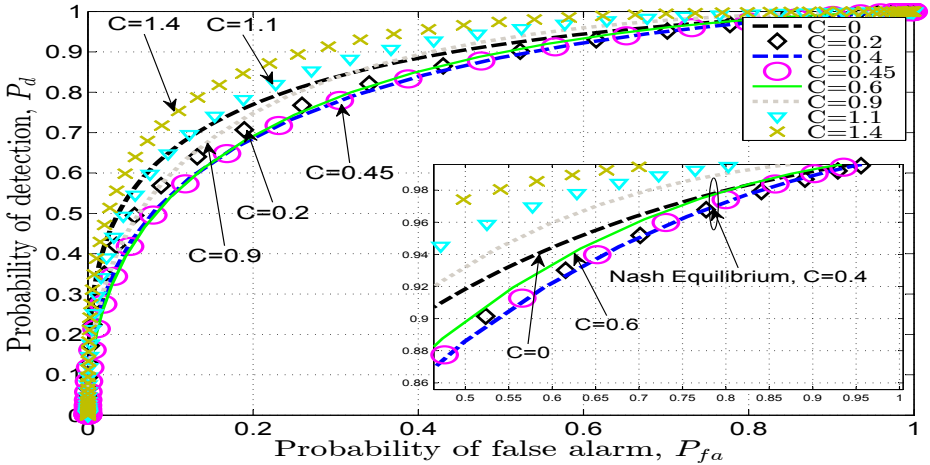

Figure 18: Probability of detection (P_d) versus probability of false alarm (P_{fa}), with $U = 3$, $\xi_a = -10.5$ dB, $P_t = 60$, $M = 12$, $N = 20$, $\beta = 0.2$, $\sigma^2_{e_h} = 0$ and with optimum weights in (6.2.22).

5. Simulation Results 4/4

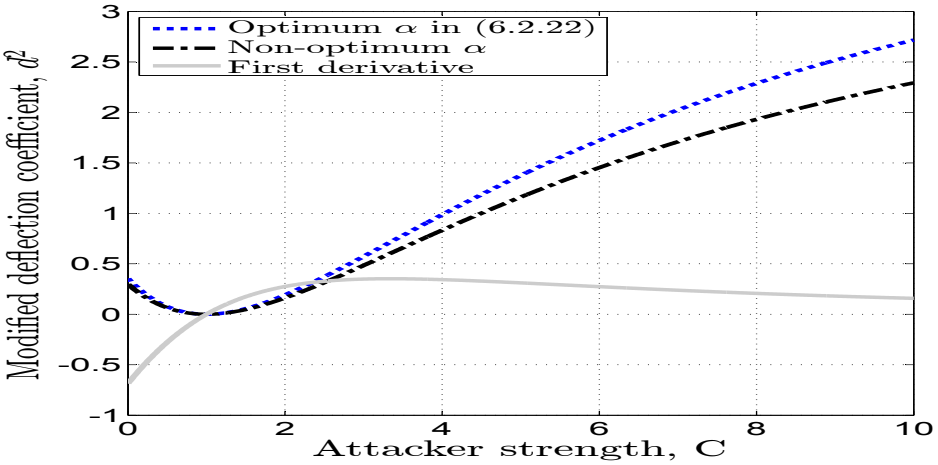

Figure 19: Modified deflection coefficient ($\tilde{d}^2$) versus the attacker strength (C) with $U = 3$, $\xi_a = -10$ dB, $s_i = 0.1, \forall i$, $P_t = 60$, $M = 12$, $N = 20$, $\beta = 0.1$ and $\sigma^2_{e_h} = 0$.

5. A Secure Sub-optimum Detection Scheme in Under-Attack WSNs

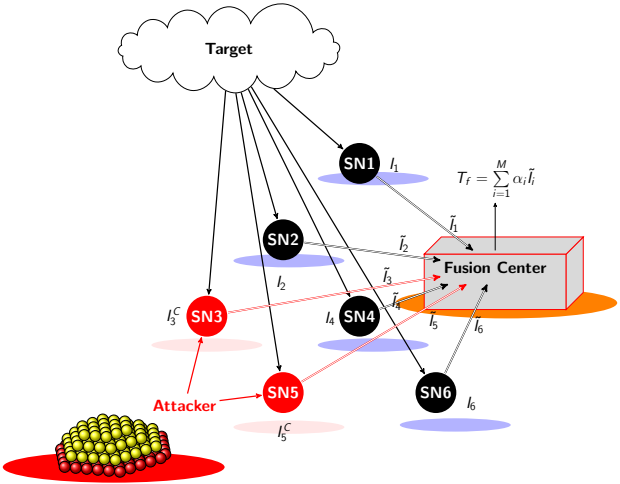

Figure 20: Under attack schematic communication architecture between peripheral SNs and the fusion center (FC). While the i^{th} ($i = \{1, 2, 4, 6\}$) honest SN indicator (test statistic) remains unchanged (i.e., $\tilde{l}_i = l_i$), the j^{th} ($j = \{3, 5\}$) compromised SN falsify its indicator (test statistic) as in (6.3.7) before transmitting to the FC.

5. A Secure Sub-optimum Detection Scheme in Under-Attack WSNs

FC Optimum Weighting

$$\alpha_{opt}^{i} = \frac{(1-\beta)\left(p_d^i - p_{fa}^i\right) + \beta\left(p_{fa}^{i,C} - p_d^{i,C}\right)\left(2P_C^{fal} - 1\right)}{(1-\beta)\left(p_d^i(1-p_d^i)\right) + \beta\left(P_C^{flip} + p_d^{i,C}\left(1-2P_C^{flip}\right)\right)\left(1-P_C^{flip} + p_d^{i,C}\left(2P_C^{flip}-1\right)\right)}. \quad (1)$$

Depends upon the local p_{fa}^i and the p_d^i as well as on the β (fraction of compromised SNs) and the probability of flipping the local decisions by the attacker. The FC cannot implement the optimum weight combining fusion rule

Attacker Flipping Probability Optimisation

Lemma 6.3.2: The optimum flipping probability $\left(P_{C,opt}^{flip}\right)$ which minimizes the modified deflection coefficient is:

$$P_{C,opt}^{flip} = \frac{\beta - 1}{2\beta}\left(\frac{\sum_{i=1}^{M}\alpha_i\left(p_d^i - p_{fa}^i\right)}{\sum_{i=1}^{M}\alpha_i\left(p_{fa}^{i,C} - p_d^{i,C}\right)}\right) + \frac{1}{2} \quad (2)$$

5. Simulation Results 1/6

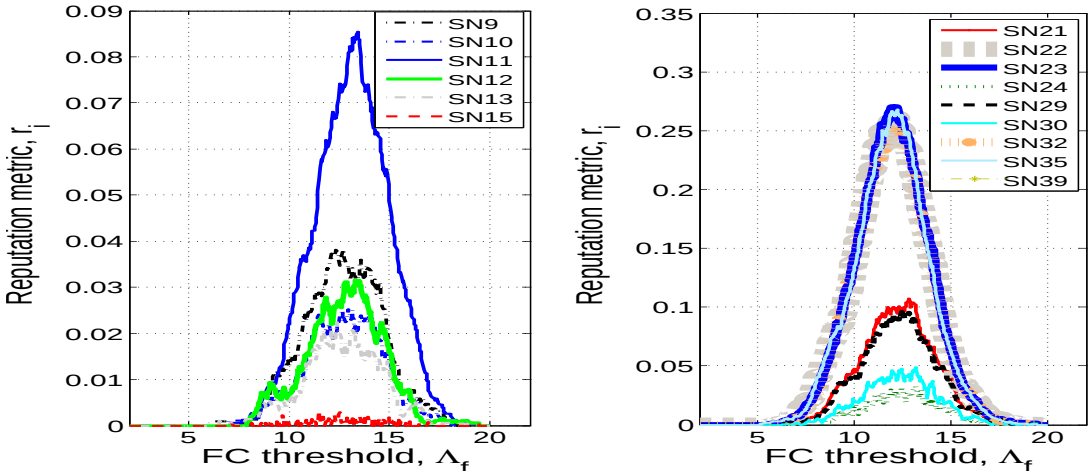

Figure 21: The reliability metric (r_i) versus the FC detection threshold (Λ_f) against the SNs with $M = 40$, $N = 20$, $\beta = 0.5$, $P_C^{flip} = 1$ and $K = 150$.

5. Simulation Results 2/6

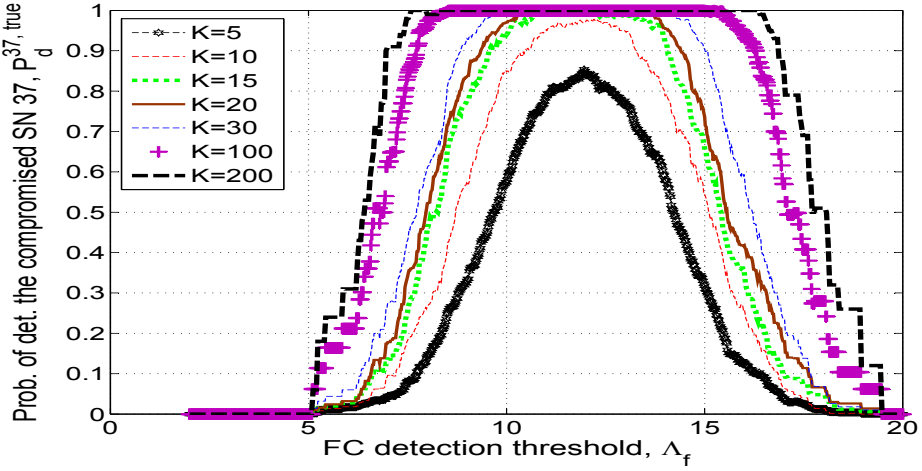

Figure 22: Probability that the (compromised) SN 37 has been truly detected ($P_d^{37,true}$) versus the FC detection threshold (Λ_f) with $M = 40$, $N = 20$, $\beta = 0.5$, $P_C^{flip} = 1$ and $\delta = 0.009$.

5. Simulation Results 3/6

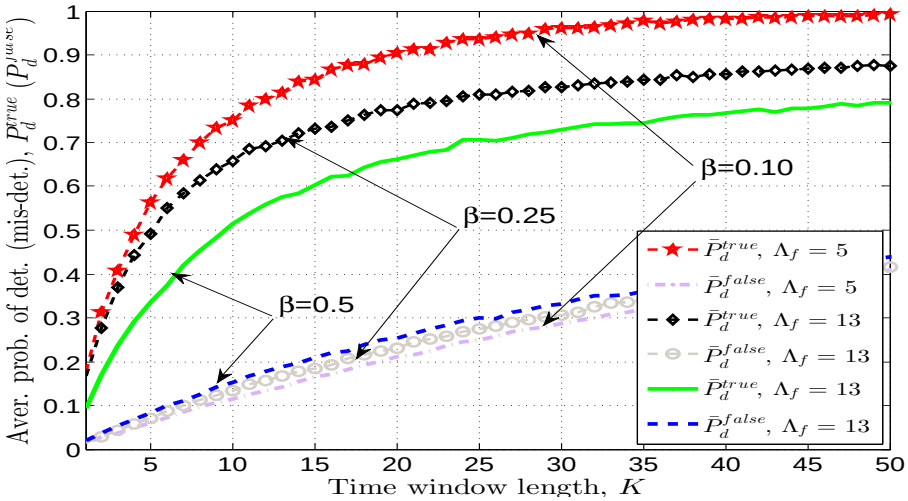

Figure 23: Average compromised SNs detection probability and honest SNs mis-detection probability versus the time window length (K) and against β with $M = 40$, $N = 20$, $P_C^{flip} = 1$ and $\delta = 0.009$.

5. Simulation Results 4/6

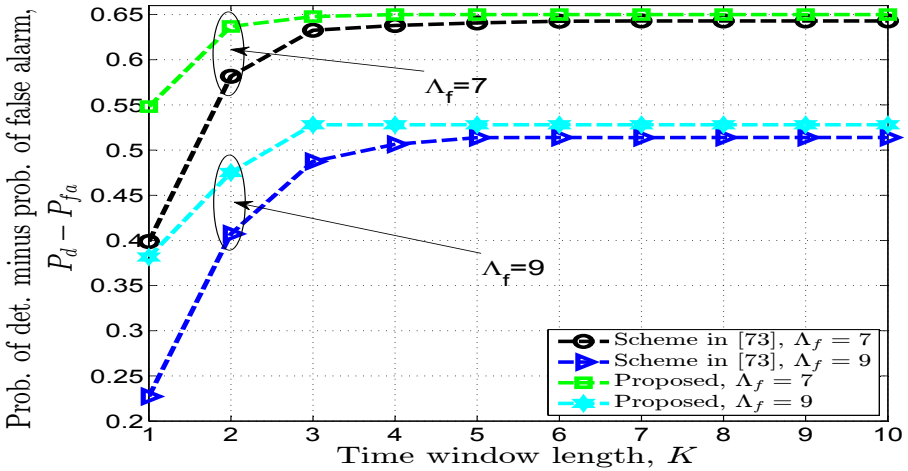

Figure 24: The $P_d - P_{fa}$ metric versus the time window length (K) against the FC detection threshold (Λ_f) with $M = 40$, $N = 20$, $\beta = 0.25$, $P_C^{flip} = 0.2$, $\delta = 0.95$ and $\mu = 10$.

5. Simulation Results 5/6

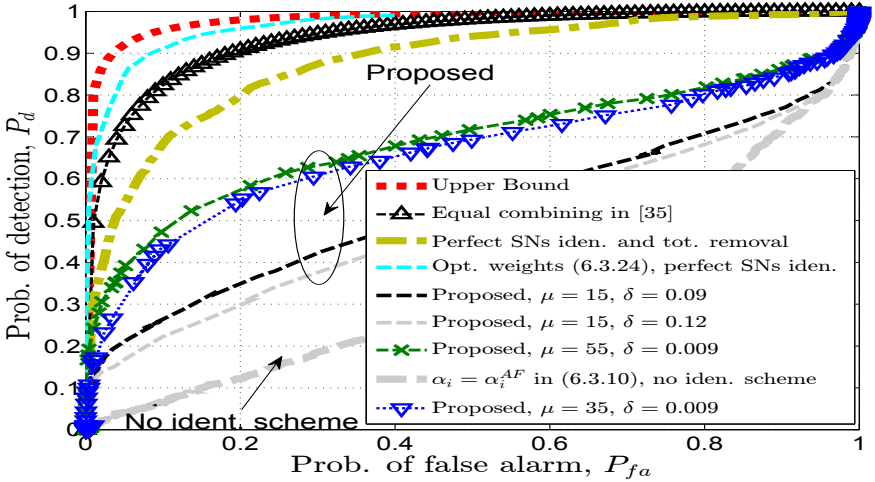

Figure 25: Probability of detection (P_d) versus probability of false alarm (P_{fa}) with $M = 40$, $N = 20$, $\beta = 0.5$, $P_C^{flip} = 1$ and $K = 5$.

5. Simulation Results 6/6

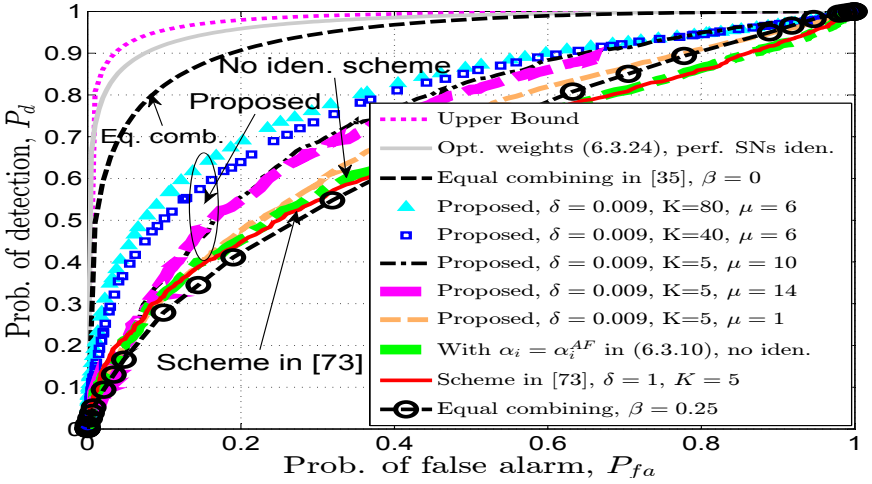

Figure 26: Probability of detection (P_d) versus probability of false alarm (P_{fa}) against δ and μ with $M = 40$, $N = 20$, $\beta = 0.25$, and $P_C^{flip} = 1$.

Summary

- We derive the optimum fusion rule and then analyze sub-optimum fusion rules that are realizable and easily implemented in practical WSN deployment scenarios. The effect of fading channels on detection performance is minimized by solving the resource allocation problem.

Summary

- We derive the optimum fusion rule and then analyze sub-optimum fusion rules that are realizable and easily implemented in practical WSN deployment scenarios. The effect of fading channels on detection performance is minimized by solving the resource allocation problem.

- A two-step consensus-based approach with weight combining quantized test statistics exchange is proposed. We relate the communication topology with the number of bits to be shared among SNs. It turns out that there is an optimum topology that maximizes the detection performance.

Summary

- We derive the optimum fusion rule and then analyze sub-optimum fusion rules that are realizable and easily implemented in practical WSN deployment scenarios. The effect of fading channels on detection performance is minimized by solving the resource allocation problem.

- A two-step consensus-based approach with weight combining quantized test statistics exchange is proposed. We relate the communication topology with the number of bits to be shared among SNs. It turns out that there is an optimum topology that maximizes the detection performance.

- Centralized detection in the presence of compromised SNs is also investigated. Attacker and FC based parameter optimization are considered and some expressions have been derived. A reputation based scheme to identify the compromised SNs in the network and control their influence to the global FC decision is also proposed.

Key Conclusions

- Shown that spatially distributed SNs across the field can offer a reliable operation for event detection applications. The system detection performance and the WSN's operating lifetime can be further improved by means of resource allocations, optimisation and signal processing algorithms

Key Conclusions

- Shown that spatially distributed SNs across the field can offer a reliable operation for event detection applications. The system detection performance and the WSN's operating lifetime can be further improved by means of resource allocations, optimisation and signal processing algorithms $\Longrightarrow$ complexity to be kept as simple as possible.

Key Conclusions

- Shown that spatially distributed SNs across the field can offer a reliable operation for event detection applications. The system detection performance and the WSN's operating lifetime can be further improved by means of resource allocations, optimisation and signal processing algorithms $\Longrightarrow$ complexity to be kept as simple as possible.
- The data fusion problem: we derive the optimal fusion rules (i.e., for attack-free and under-attack WSN scenarios) and have shown that these fusion rules are not implementable in practice and require complex local signal processing

Key Conclusions

- Shown that spatially distributed SNs across the field can offer a reliable operation for event detection applications. The system detection performance and the WSN's operating lifetime can be further improved by means of resource allocations, optimisation and signal processing algorithms $\Longrightarrow$ complexity to be kept as simple as possible.
- The data fusion problem: we derive the optimal fusion rules (i.e., for attack-free and under-attack WSN scenarios) and have shown that these fusion rules are not implementable in practice and require complex local signal processing $\Longrightarrow$ Derive sub-optimum but simple fusion rules (requiring simple hardware) that offer reliable and good detection performance.

Key Conclusions

- Shown that spatially distributed SNs across the field can offer a reliable operation for event detection applications. The system detection performance and the WSN's operating lifetime can be further improved by means of resource allocations, optimisation and signal processing algorithms $\Longrightarrow$ complexity to be kept as simple as possible.
- The data fusion problem: we derive the optimal fusion rules (i.e., for attack-free and under-attack WSN scenarios) and have shown that these fusion rules are not implementable in practice and require complex local signal processing $\Longrightarrow$ Derive sub-optimum but simple fusion rules (requiring simple hardware) that offer reliable and good detection performance.
- A better but more complex approach is to possibly identify these compromised SNs and control their influence on the FC decision

Key Conclusions

- Shown that spatially distributed SNs across the field can offer a reliable operation for event detection applications. The system detection performance and the WSN's operating lifetime can be further improved by means of resource allocations, optimisation and signal processing algorithms $\Longrightarrow$ complexity to be kept as simple as possible.
- The data fusion problem: we derive the optimal fusion rules (i.e., for attack-free and under-attack WSN scenarios) and have shown that these fusion rules are not implementable in practice and require complex local signal processing $\Longrightarrow$ Derive sub-optimum but simple fusion rules (requiring simple hardware) that offer reliable and good detection performance.
- A better but more complex approach is to possibly identify these compromised SNs and control their influence on the FC decision $\Longrightarrow$ Offers an improved detection performance but requires observing the SN's local reports for a period of time. A larger observation time period (K) may lead to a large detection delay that is critical for most of the event detection applications.

Key Conclusions

- Shown that spatially distributed SNs across the field can offer a reliable operation for event detection applications. The system detection performance and the WSN's operating lifetime can be further improved by means of resource allocations, optimisation and signal processing algorithms $\Longrightarrow$ complexity to be kept as simple as possible.
- The data fusion problem: we derive the optimal fusion rules (i.e., for attack-free and under-attack WSN scenarios) and have shown that these fusion rules are not implementable in practice and require complex local signal processing $\Longrightarrow$ Derive sub-optimum but simple fusion rules (requiring simple hardware) that offer reliable and good detection performance.
- A better but more complex approach is to possibly identify these compromised SNs and control their influence on the FC decision $\Longrightarrow$ Offers an improved detection performance but requires observing the SN's local reports for a period of time. A larger observation time period (K) may lead to a large detection delay that is critical for most of the event detection applications.
- We have addressed the fully distributed detection problem and proposed signal processing algorithms for such an approach

Key Conclusions

- Shown that spatially distributed SNs across the field can offer a reliable operation for event detection applications. The system detection performance and the WSN's operating lifetime can be further improved by means of resource allocations, optimisation and signal processing algorithms $\Longrightarrow$ complexity to be kept as simple as possible.
- The data fusion problem: we derive the optimal fusion rules (i.e., for attack-free and under-attack WSN scenarios) and have shown that these fusion rules are not implementable in practice and require complex local signal processing $\Longrightarrow$ Derive sub-optimum but simple fusion rules (requiring simple hardware) that offer reliable and good detection performance.
- A better but more complex approach is to possibly identify these compromised SNs and control their influence on the FC decision $\Longrightarrow$ Offers an improved detection performance but requires observing the SN's local reports for a period of time. A larger observation time period (K) may lead to a large detection delay that is critical for most of the event detection applications.
- We have addressed the fully distributed detection problem and proposed signal processing algorithms for such an approach $\Longrightarrow$ Very attractive from both the signal processing perspective and the communication point of view.

Questions/Comments